IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Art Unit: 2135

Kenneth L. Levy Conf. No.: 2246

Application No.: 10/622,180

Filed: July 16, 2003 **Via Electronic Filing**

For: Digital Watermarking and Fingerprinting Applications for Copy Control

Examiner: B. TO

Date: August 29, 2008

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellant respectfully requests the Board of Patent Appeals and Interferences (hereafter the "Board") to *reverse* the outstanding final rejection of the pending claims.

This Appeal Brief is in furtherance of a Notice of Appeal filed April 30, 2008. Please charge the fee required under 37 CFR 1.17(f) and any other fees needed to consider this Appeal Brief to our deposit account no. 50-1071.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is Digimarc Corporation, by an assignment from the inventor recorded at Reel 014671, frames 0433-0434, on November 5, 2003.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 1-39 and 41-48 are pending in the present application. Each of the pending claims stands finally rejected.

Claim 40 was previously canceled.

STATUS OF AMENDMENTS

All earlier-filed amendments have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The pending claims relate generally to copy protection for audio, video and image content.

For example, claim 18 recites a method of providing copy protection for protected media content on a computer system. The computer system includes an output port and an associated output buffer, and an input port and an associated input buffer [see, e.g., Fig. 2, items 110 and 120; see also page 8, lines 15-18]. The method includes: analyzing first media content buffered in the output buffer; analyzing second media content buffered in the input buffer; and comparing the first media content buffered in the output buffer with the second media content buffered in the input buffer [see, e.g., page 8, line 24 – page 10, line 14; see also Fig. 2, items 130 and/or 140]. A copy operation is modified or disabled when the first media content and the second media content match or otherwise coincide [see, e.g., Fig. 2, items 140 and/or 150; see also page 10, 13-22].

Claim 33 recites a method of providing copy protection for protected media content on a computer system, the computer system comprising an output port and an associated output buffer, and an input port and an associated input buffer [see, e.g., Fig. 2, items 110 and 120; see also page 8, lines 15-18]. The method includes: obtaining first media content buffered in the output buffer; obtaining second media content buffered in the input buffer; and comparing the first media content buffered in the output buffer and the second media content buffered in the input buffer through correlation of the first media content with the second media content [see, e.g., page 8, line 24 – page 10, line 14; see also Fig. 2, items 130 and/or 140]. A copy operation is modified or disabled when the correlation of the first media content and the second media content indicates that the first media content and the second media content match or otherwise coincide[see, e.g., Fig. 2, items 140 and/or 150; see also page 10, 13-22].

Claim 48 recites a method of providing copy control for protected media content, the protected media content comprising a digital watermark embedded therein according to a key. The digital watermark includes a payload. The method includes: determining which out of a plurality of copy control states should govern the protected media content by reference to the watermark key [see, e.g., page 12, lines 9-12 and lines 13-24]; determining which out of a plurality of copy control systems the content should be handled by reference to the watermark payload [see, e.g., page 13, lines 6-13]; and providing copy control according to the determined copy control state through the determined copy control system [see, e.g., page 12, line 6 – page 14, line 29].

Claim 39 recites a method of providing copy control for protected media content including: determining which out of a plurality of copy control systems applies to the protected media content, said protected media content comprises a digital watermark embedded therein according to a key [see, e.g., page 12, lines 13-24], said determining determines which out of a plurality of copy control systems applies to the protected media content based on the key [see, e.g., page 12, lines 9-12 and lines 13-24]; and controlling the protected media content according to a determined copy control system [see, e.g., page 12, line 6 – page 14, line 29].

Claim 1 recites a method of copy protecting media content including [see, e.g., Fig. 1 and page 5, line 25 – page 8, line 10]: determining whether the media content is designated as copy once [see, e.g., page 5, line 26 – page 6, line 5; see also Fig. 1, item 200]; if the media content is designated as copy once, obtaining an identifier for the media content [see, e.g., page 6, lines 7-24; see also Fig. 1, item 210]; querying a data repository – which is separate from the media content itself – to determine if the identifier is stored therein [see, e.g., Fig. 1, item 220; see also page 6, line 25 – page 7, line 23]; if the identifier is found in the data repository, modifying or disabling a copy function [see, e.g., page 7, lines 17-21; see also Fig. 1, item 230]; and if the identifier is not found in the data repository, adding the identifier to the data repository [see, e.g., Fig. 1, item 240; see also page 7, lines 22-23].

Claim 17 recites a recording device that is operable to copy media content [see, e.g., page 7, lines 4-16; see also page 15, line 27 – page 16, lines 5]. The device includes: a data repository [see, e.g., page 7, lines 4-16 and page 16, lines 3-5]; electronic processing circuitry [see, e.g., page 7, lines 4-16; see also page 15, line 27 – page 16, lines 5]; a system communications bus to facilitate communication between the data repository and the electronic processing circuitry [see, e.g., page 7, lines 4-16; see also page 15, line 27 – page 16, lines 5; see also original claim 17]. The electronic processing circuitry executes acts of: determining whether media content – which is separate from the data repository – is designated as copy once [see, e.g., page 5, line 26 – page 6, line 5; see also Fig. 1, item 200]; if the media content is designated as copy once, obtaining an identifier for the media content [see, e.g., page 6, lines 7-24; see also Fig. 1, item 210]; querying the data repository to determine if the identifier is stored therein [see, e.g., Fig. 1, item 220; see also page 6, line 25 – page 7, line 23]; if the identifier is stored in the data repository, modifying or disabling a copy function [see, e.g., page 7, lines 17-21; see also Fig. 1, item 230]; and if the identifier is not stored in the data repository, storing the identifier to the data repository [see, e.g., Fig. 1, item 240; see also page 7, lines 22-23].

(Of course, additional specification support can be found throughout the application as filed. Thus, citations to specific page and line numbers are by way of example and should not limit specification support or claim scope.)

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 18-28 and 32-38[1] stand finally rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,850,252 (hereafter referred to as "the Hoffberg Patent" or simply as "Hoffberg").

2. Claims 1-17, 39, 41, 42 and 45-48 stand finally rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Publication No. US 2001-0042043 A1 (hereafter referred to as "the Shear publication" or simply as "Shear").

ARGUMENT

Rejections under U.S.C. 102(e) over Hoffberg

Claim 18

Independent claim 18 recites:

18. *A method of providing copy protection for protected media content on a computer system, the computer system comprising an output port and an associated output buffer, and an input port and an associated input buffer, said method comprising:*

analyzing first media content buffered in the output buffer;

analyzing second media content buffered in the input buffer; and

comparing the first media content buffered in the output buffer with the second media content buffered in the input buffer, wherein a copy operation is modified or disabled when the first media content and the second media content match or otherwise coincide.

---

1 The rejection heading on page 14, paragraph 6, of the final Office Action erroneously states that claims 18-32 are rejected over Hoffberg. Indeed, the final Office Action appears to reject claims 18-28 and 32-38 over Hoffberg. Please see the final Office Action, pages 19-21.

Hoffberg does not have each and every limitation of claim 18; namely, it does not: i) compare content buffered in an output buffer with content buffered in an input buffer; and ii) modify or disable a copy operation when the first media content and the second media content match or otherwise coincide.

It is well settled that in order for an Examiner to establish a *prima facie* case of anticipation, each and every element of the claimed invention, arranged as required by the claim, must be found in a single prior art reference, either expressly or under the principles of inherency. *See generally*, In re Schreiber, 128 F.3d 1473, 1477 (Fed. Cir. 1997); Diversitech Corp. v. Century Steps, Inc., 850 F.2d 675, 677-78 (Fed. Cir. 1988); Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick, 730 F.2d 1452, 1458 (Fed. Cir. 1984).

Hoffberg does not anticipate claim 18 because it does not include – either expressly or inherently – at least: i) comparing content buffered in an output buffer with content buffered in an input buffer; and ii) modifying or disabling a copy operation when the first media content and the second media content match or otherwise coincide.

The Office Action points to Hoffberg's abstract, Col. 113, lines 30-34 and 54-63, and Col. 121, lines 14-30 as teaching the above acts. *Please see* the final Office Action, page 15. We respectfully disagree with the final Office Action for at least the three (3) reasons set forth below. The cited Hoffberg passages are reproduced immediately below for the Board's convenience and easy reference.

Abstract:

An intelligent electronic appliance preferably includes a user interface, data input and/or output port, and an intelligent processor. A preferred embodiment comprises a set top box for interacting with broadband media streams, with an adaptive user interface, content-based media processing and/or media metadata processing, and telecommunications integration. An adaptive user interface models the user, by observation, feedback, and/or explicit input, and presents a user interface and/or executes functions based on the user model. A content-based media processing system analyzes media content, for example audio and video, to understand the content, for example to generate content-descriptive metadata. A media metadata processing system operates on locally

or remotely generated metadata to process the media in accordance with the metadata, which may be, for example, an electronic program guide, MPEG 7 data, and/or automatically generated format. A set top box preferably includes digital trick play effects, and incorporated digital rights management features.

Column 113, lines 30-34 and 54-63:

The interface system according to the present invention is not limited to a single data source, and may analyze data from many different sources for its operation. This data may be stored data or present in a data stream. Thus, in a multimedia system, there may be a real-time data stream....

....

A fractal-based system includes a database of image objects, which may be preprocessed in a manner which makes them suitable for comparison to a fractal-transformed image representation of an image to be analyzed. Thus, corresponding "fractal" transforms are performed on the unidentified image or a portion thereof and on an exemplar of a database. A degree of relatedness is determined in this "fractal transform domain", and the results used to identify objects within the image. The system then makes decisions based on the information content of the image, i.e. the objects contained therein.

Column 121, lines 14-30:

The first element in the content protection scheme is the copy control information (CCI). CCI is a way for content owners to specify how their content can be used. Some examples are "copy never," "copy once," "no more copies," and "copy free." The content protection system is capable of securely communicating copy control information between devices. Two different CCI mechanisms are supported and are discussed below. In the event that conflicting copy protection requirements are specified by the different mechanisms, sink devices should follow the most restrictive CCI available. Embedded CCI is carried as part of the content stream. Many content formats (including MPEG) have fields allocated for carrying the CCI associated with the stream. The integrity of the embedded CCI is ensured since tampering with the content stream results in erroneous decryption of the content.

First, the above quoted Hoffberg passages say nothing about comparing content buffered in an output buffer with content buffered in an input buffer. In this regard, reference to Hoffberg's abstract stating a presence of input/output ports in a system does not teach comparing content in such input/output ports.

Second, the cited Col. 113, lines 54-58, passage deals with a database of image objects; it is highly unlikely that the interface system discussed in the Hoffberg patent would store a database of image objects in an input or output *buffer*, since buffers are routinely reset, overwritten or purged. The database would be stored in a more permanent form, e.g., a CD-ROM or on-line database accessible through a serial data link. *See* Hoffberg, Col. 114, lines 5-8. Thus, the cited Hoffberg passages are not applicable to the combination recited in claim 18.

Third, while the cited Hoffberg Col. 121, lines 14-30, passage discusses copy control information (CCI) carried with content (e.g., MPEG video), it says nothing about modifying or disabling a copy operation when the content in an output buffer matches or otherwise coincides with content in an input buffer. Moreover, the reference to "*a degree of relatedness*" mentioned at Col. 113 (and cited in the final Office Action, page 15, last two lines) is concerned with identifying an object within an image (see Hoffberg, Col. 113, lines 60-62) and not modifying or disabling a copy operation. Thus, the statements in the cited Col. 113 passage seem incongruently combined with the statements in the cited Col. 121 passage.

We respectfully request that the final rejection of claim 18 be withdrawn since Hoffberg does not have each and every feature of claim 18; namely, Hoffberg does not: i) compare content buffered in an output buffer with content buffered in an input buffer; and ii) modify or disable a copy operation when the first media content and the second media content match or otherwise coincide.

Claim 33

Independent claim 33 recites:

33. A method of providing copy protection for protected media content on a computer system, the computer system comprising an output port and an associated output buffer, and an input port and an associated input buffer, said method comprising:

obtaining first media content buffered in the output buffer;

obtaining second media content buffered in the input buffer; and

comparing the first media content buffered in the output buffer and the second media

content buffered in the input buffer through correlation of the first media content with the second media content, wherein a copy operation is modified or disabled when the correlation of the first media content and the second media content indicates that the first media content and the second media content match or otherwise coincide.

> *Hoffberg does not have each and every limitation of claim 33; namely, it does not i) compare first media content buffered in an output buffer and second media content buffered in an input buffer through correlation of the first media content with the second media content, and ii) modify or disable a copy operation when the correlation of the first media content and the second media content indicates that the first media content and the second media content match or otherwise coincide.*

To establish a *prima facie* case of anticipation, each and every element of the claimed invention, arranged as required by the claim, must be found in a single prior art reference, either expressly or under the principles of inherency. *See generally*, In re Schreiber, 128 F.3d 1473, 1477 (Fed. Cir. 1997); Diversitech Corp. v. Century Steps, Inc., 850 F.2d 675, 677-78 (Fed. Cir. 1988); Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick, 730 F.2d 1452, 1458 (Fed. Cir. 1984).

Hoffberg does not anticipate claim 33 because it does not include – either expressly or inherently – at least: i) comparing first media content buffered in an output buffer and second media content buffered in an input buffer through correlation of the first media content with the second media content, and ii) modifying or disabling a copy operation when the correlation of the first media content and the second media content indicates that the first media content and the second media content match or otherwise coincide.

The Office Action points to Hoffberg's abstract, Col. 113, lines 30-34 and 54-58, Col. 121, lines 14-30, and Col. 171, lines 23-30, as teaching the above acts. We respectfully disagree for at least the following four (4) reasons. (The cited Hoffberg passages are quoted above on pages 7 and 8 of this Appeal Brief.)

First, the cited Hoffberg passages say nothing about comparing content buffered in an output buffer with content buffered in an input buffer. In this regard, reference to Hoffberg's

abstract stating a presence of input/output ports in a system does not teach comparing content in input/output ports.

Second, the cited Col. 113, lines 54-58, passage deals with a database of image objects; it is highly unlikely that the interface system discussed in the Hoffberg patent would store a database of image object in an input or output buffer, since buffers are routinely reset, overwritten or purged. The database would be stored in a more permanent form, e.g., a CD-ROM or on-line database accessible through a serial data link. See, e.g., Hoffberg at Col. 114, lines 5-8.

Third, while the cited Col. 121, lines 14-30, passage discusses copy control information (CCI) carried with content (e.g., MPEG video), it says nothing about modifying or disabling a copy operation when the content in an output buffer matches or otherwise coincides with content in an input buffer. Moreover, the reference to "a degree of relatedness" mentioned at Col. 113, lines 60-61 (and relied on in the final Office Action, page 20, lines 1-3) is concerned with *identifying* an object within an image (see Hoffberg, Col. 113, lines 60-62) and not modifying or disabling a copy operation. Thus, the statements in the cited Col. 113 passages seem incongruently combined with the statements in the cited Col. 121 passage.

Fourth, the cited Col. 172 passage does not have a nexus with copy control, as recited in claim 33. This Hoffberg passage is reproduced below.

> *These optical recognition systems are best suited to applications where an uncharacterized input signal frame is to be compared to a finite number of visually different comparison frames (i.e., at least one, with an upper limit generally defined by the physical limitations of the optical storage media and the system for interfacing to the storage media), and where an optical correlation will provide useful information.*

Indeed, the above quoted passage does not have a nexus with copy control. Like the cited Col. 113 passage, the cited Col. 172 passage seems incongruently combined with the statement in the Col. 121 passage.

We respectfully request that the final rejection of claim 33 be reversed since Hoffberg fails to disclose each and every feature recited in claim 33; namely, Hoffberg does not have at

least: i) comparing first media content buffered in an output buffer and second media content buffered in an input buffer through correlation of the first media content with the second media content, and ii) modifying or disabling a copy operation when the correlation of the first media content and the second media content indicates that the first media content and the second media content match or otherwise coincide.

Rejections under U.S.C. 102(e) over Shear

Claim 48

Independent claim 48 recites:

48. A method of providing copy control for protected media content, the protected media content comprising a digital watermark embedded therein according to a key, said digital watermark comprising a payload, said method comprising:

determining which out of a plurality of copy control states should govern the protected media content by reference to the watermark key;

determining which out of a plurality of copy control systems the content should be handled by reference to the watermark payload; and

providing copy control according to the determined copy control state through the determined copy control system.

Shear does not have each and every limitation of claim 48; namely, determining which out of a plurality of copy control states should govern the protected media content by reference to a watermark key.

Claim 48 refers to both a watermark "key" and a watermark "payload." The watermark payload conveys or carries a message or information, e.g., plural-bit data. The Shear publication's control codes (paragraph 62) and comprehensive rights management information (paragraph 283) comprise data that may be included in a watermark *payload*.

The same can not be said for a watermark *key*.

In the context of this claim, a watermark key reveals some secret or information about a watermark embedding or decoding process. For example, the subject specification teaches and describes on page 9, lines 18-24:

> *For example, the key reveals information about a watermarking protocol, a watermark embedding/decoding characteristic and/or a watermark payload encryption key. In one implementation a key provides a pseudo-random sequence that is used to embed the watermark. In another example, a key specifies locations for watermark embedding, host signal features to be modified to effect embedding, and/or semantic meaning of particular features (e.g., how modifications to the host signal are mapped to particular data symbols, such as binary or M-ary symbols), etc., etc.*

Of course, other examples will fall within the scope of this claim.

The cited passages in the Shear publication (namely, paragraph [0218], [0220] and [0270]) do not teach both a watermark payload and key as used in this claim. In particular, the cited passages in the Shear publication do not teach at least determining which out of a plurality of *copy control states* should govern protected media content *by reference to a watermark key*.

For example, while the relied upon Shear paragraph [0218] (please see the final Office Action, page 13, lines 3-6) discusses decryption keys, there is nothing in this passage that discusses "determining which out of a plurality of copy control states should govern the protected media content by reference to the **watermark** key."

Shear's "hidden key, element 210" is carried on a disk 100 to assist in decrypting content stored on the disk. Carrying a decryption key on a disk is not determining a copy control state by reference to a watermark key, as recited in claim 48.

We respectfully request that the final rejection of claim 48 be reversed since Shear does not have each and every element of claim 48; namely Shear lacks at least determining which out of a plurality of copy control states should govern the protected media content by reference to the watermark key.

Claim 39

Independent claim 39 recites:

39. A method of providing copy control for protected media content comprising:

determining which out of a plurality of copy control systems applies to the protected media content, said protected media content comprises a digital watermark embedded therein according to a key, said determining determines which out of a plurality of copy control systems applies to the protected media content based on the key; and

controlling the protected media content according to a determined copy control system.

To establish a *prima facie* case of anticipation, each and every element of the claimed invention, arranged as required by the claim, must be found in a single prior art reference, either expressly or under the principles of inherency. *See generally*, In re Schreiber, 128 F.3d 1473, 1477 (Fed. Cir. 1997); Diversitech Corp. v. Century Steps, Inc., 850 F.2d 675, 677-78 (Fed. Cir. 1988); Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick, 730 F.2d 1452, 1458 (Fed. Cir. 1984).

Shear does not anticipate claim 39 because it does not include – either expressly or inherently – at least determining which out of a plurality of copy control systems applies to the protected media content based on a digital watermarking key, in combination with other features of claim 39.

The cited Shear passage, paragraph [0218] (*see* the final Office Action, page 12, lines 10-13), discusses a decryption key carried on a disk. But there is no discussion in this passage of determining a copy control system to apply to protected media content based on a digital watermark key.

Moreover, the final Office Action erroneously suggests that element 210 in Fig. 3 is somehow related to a digital watermarking key. Please see the final Office Action, page 12, lines 8-9. Element 210 is a decryption key used to decrypt content carried on a DVD disk 100. Please see Shear at paragraph [0218]. There is no nexus between Shear's cited decryption key 210 and

any watermarking key, let alone a nexus between the decryption key 210 and determining a copy control system to apply to protected media content (based on a digital watermarking key).

We respectfully request that the final rejection of claim 39 be withdrawn since Shear does not have each and every limitation of claim 39; including, determining which out of a plurality of copy control systems applies to the protected media content based on a digital watermark key.

Claim 1

Independent claim 1 recites:

1. A method of copy protecting media content comprising:

determining whether the media content is designated as copy once;

if the media content is designated as copy once, obtaining an identifier for the media content;

querying a data repository – which is separate from the media content itself – to determine if the identifier is stored therein;

if the identifier is found in the data repository, modifying or disabling a copy function; and

if the identifier is not found in the data repository, adding the identifier to the data repository.

To establish a *prima facie* case of anticipation, each and every element of the claimed invention, arranged as required by the claim, must be found in a single prior art reference, either expressly or under the principles of inherency. *See generally,* In re Schreiber, 128 F.3d 1473, 1477 (Fed. Cir. 1997); Diversitech Corp. v. Century Steps, Inc., 850 F.2d 675, 677-78 (Fed. Cir. 1988); Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick, 730 F.2d 1452, 1458 (Fed. Cir. 1984).

Shear does not anticipate claim 1 because it does not include – either expressly or inherently –acts of: querying a data repository – *which is separate from the media content itself* – to determine if the identifier is stored therein, and *if the identifier is not found in the data*

repository, adding the identifier to the data repository.

The cited passage of the Shear publication (paragraph [0254]) does not have the *conditioned nature* of claim 1, e.g., "**if** the identifier is **not** found in the data repository, adding the identifier to the data repository." The cited Shear paragraph [0254] is provided below for the Board's convenience:

> *[0254] As a further example, the player 52 can be programmed to place a copy it makes of a digital property such as a film in encrypted form inside a tamper-resistant software container. The software container may carry with it a code indicating that the digital property is a copy rather than an original. The sending player 52 may also put its own unique identifier (or the unique identifier of an intended receiving device such as another player 52, a video cassette player or equipment 50) in the same secure container to enforce a requirement that the copy can be played only on the intended receiving device. Player 52 (or other receiving device) can be programmed to make no copies (or no additional copies) upon detecting that the digital property is a copy rather than an original. If desired, a player 52 can be programmed to refuse to play a digital property that is not packaged with the player's unique ID.*

This paragraph does not have "if the identifier is not found in the data repository, adding the identifier to the data repository," as recited in claim 1.

Claim 1 also recites that a queried data repository is separate from the media content. In contrast, the cited Shear paragraph [0254] (quoted above) points to a software or encryption container. This does not show a separate data repository and media content.

Thus, we respectfully request that the final rejection of claim 1 be reversed since Shear does not have each and every feature of claim 1; namely, Shear does not have at least acts of: querying a data repository – *which is separate from the media content itself* – to determine if the identifier is stored therein, and *if the identifier is not found in the data repository, adding the identifier to the data repository.*

Claim 17

Independent claim 17 recites:

17. A recording device that is operable to copy media content, said device comprising:

a data repository;

electronic processing circuitry;

a system communications bus to facilitate communication between the data repository and the electronic processing circuitry, said electronic processing circuitry executing acts of:

determining whether media content – which is separate from the data repository – is designated as copy once;

if the media content is designated as copy once, obtaining an identifier for the media content;

querying the data repository to determine if the identifier is stored therein;

if the identifier is stored in the data repository, modifying or disabling a copy function; and

if the identifier is not stored in the data repository, storing the identifier to the data repository.

Claim 17 recites features that are analogous to those discussed above with respect to claim 1. The rejection of claim 17 should be reversed for at least the reasons noted above with respect to claim 1.

CONCLUSION AND REQUEST FOR REVERSAL

Appellant respectfully requests reversal of the final rejection of the pending claims.

Respectfully submitted,

Date: August 29, 2008

DIGIMARC CORPORATION

Customer No. 23735

By: /Steven W. Stewart, Reg. No. 45,133/
Steven W. Stewart
Registration No. 45,133

Telephone: 503-469-4685
FAX: 503-469-4777

CLAIMS APPENDIX

1. (previously presented): A method of copy protecting media content comprising:

determining whether the media content is designated as copy once;

if the media content is designated as copy once, obtaining an identifier for the media content;

querying a data repository – which is separate from the media content itself – to determine if the identifier is stored therein;

if the identifier is found in the data repository, modifying or disabling a copy function; and

if the identifier is not found in the data repository, adding the identifier to the data repository.

2. (original): The method of claim 1, wherein the identifier comprises a content identifier.

3. (previously presented): The method of claim 2, wherein the content identifier is conveyed by a digital watermark embedded in the media content, and said obtaining comprises reading the digital watermark to obtain the content identifier.

4. (original): The method of claim 2, wherein the content identifier is obtained from a header associated with the media content.

5. (original): The method of claim 2, wherein the content identifier is obtained from an encryption system associated with the media content.

6. (original): The method of claim 2, wherein the content identifier is obtained by determining a fingerprint of the media content.

7. (original): The method of claim 1, wherein the media content is stored on physical media, and the identifier comprises a physical media identifier.

8. (original): The method of claim 7, wherein the physical media comprises a DVD, and the physical media identifier comprises a unique serial number corresponding to the DVD.

9. (original): The method of claim 1, further comprising allowing copying of the media content when the identifier is not found in the data repository.

10. (previously presented): The method of claim 1, wherein the media content comprises a digital watermark embedded therein, the digital watermark indicating that the media content is designated as copy once, and wherein said determining comprises reading the digital watermark.

11. (previously presented): The method of claim 1, wherein the media content comprises metadata associated therewith, the metadata indicating that the media content is designated as copy once, and wherein said determining comprises analyzing the metadata.

12. (original): The method of claim 11, wherein the metadata is stored in a file header.

13. (previously presented): The method of claim 1, wherein the media content is associated with an encryption system, the encryption system indicating that the media content is designated as copy once, and wherein said determining comprises communicating with the encryption system.

14. (original): A recording device performing the method of claim 1.

15. (original): The recording device according to claim 14, wherein the data repository is co-located with the recording device.

16. (original): The recording device according to claim 14, wherein the data repository is remotely located from the recording device.

17. (previously presented): A recording device that is operable to copy media content, said device comprising:

a data repository;

electronic processing circuitry;

a system communications bus to facilitate communication between the data repository and the electronic processing circuitry, said electronic processing circuitry executing acts of:

determining whether media content – which is separate from the data repository – is designated as copy once;

if the media content is designated as copy once, obtaining an identifier for the media content;

querying the data repository to determine if the identifier is stored therein;

if the identifier is stored in the data repository, modifying or disabling a copy function; and

if the identifier is not stored in the data repository, storing the identifier to the data repository.

18. (original): A method of providing copy protection for protected media content on a computer system, the computer system comprising an output port and an associated output buffer, and an input port and an associated input buffer, said method comprising:

analyzing first media content buffered in the output buffer;

analyzing second media content buffered in the input buffer; and

comparing the first media content buffered in the output buffer with the second media content buffered in the input buffer, wherein a copy operation is modified or disabled when the first media content and the second media content match or otherwise coincide.

19. (original): The method of claim 18, wherein the computer system comprises a single computer system.

20. (original): The method of claim 19, wherein the output buffer comprises a matrix of output buffers, and the input buffer comprises a matrix of input buffers.

21. (previously presented): The method of claim 20, wherein said comparing compares at least active output buffers with active input buffers.

22. (original): The method of claim 18, wherein the computer system comprises at least two networked computers, with a first computer comprising the output port and a second computer comprising the input port.

23. (original): The method of claim 22, wherein the output buffer comprises a matrix of output buffers, and the input buffer comprises a matrix of input buffers.

24. (previously presented): The method of claim 23, wherein said comparing compares at least content buffered in active output buffers with content buffered in active input buffers.

25. (previously presented): The method of claim 18, wherein the first media content comprises a first identifier embedded therein in the form of a digital watermark and the second media content comprises a second identifier embedded therein in the form of a digital watermark, and wherein said analyzing first media content buffered in the output buffer comprises obtaining the first identifier from its watermark, said analyzing second media content buffered in the input buffer comprises obtaining the second identifier from its watermark, and said comparing the first media content buffered in the output buffer and the second media content buffered in the input buffer comprises comparing at least a portion of the first identifier with at least a portion of the second identifier.

26. (original): The method of claim 25, wherein the copy operation is modified or disabled when the portion of the first identifier and the portion of the second identifier match or otherwise coincide.

27. (previously presented): The method of claim 18, wherein the first media content comprises a first identifier embedded in the form of a digital watermark, and wherein said analyzing first media content buffered in the output buffer comprises obtaining the first identifier from its watermark, and said analyzing second media content buffered in the input buffer comprises obtaining a plurality of identifiers embedded as digital watermarks in the second media over a time period, and said comparing the first media content buffered in the output buffer and the second media content buffered in the input buffer comprises comparing at least a portion of the first identifier with at least portions of the plurality of identifiers.

28. (original): The method of claim 27, wherein the copy operation is modified or disables when the portion of the first identifier and the portions of the plurality of identifiers match or otherwise coincide.

29. (previously presented): The method of claim 18, wherein said analyzing first media content buffered in the output buffer comprises determining a first fingerprint of the first media content, said analyzing second media content buffered in the input buffer comprises determining a second fingerprint of the second media content, and said comparing the first media content buffered in the output buffer and the second media content buffered in the input buffer comprises comparing at least a portion of the first fingerprint with at least a portion of the second fingerprint.

30. (original): The method of claim 29, wherein the copy operation is modified or disabled when the portion of the first fingerprint and the portion of the second fingerprint match or otherwise coincide.

31. (original): The method of claim 29, further comprising compensating for a time delay associated with the second media content, relative to the first media content.

32. (original): The method of claim 18, further comprising determining that the media content is protected via reference to at least one of a digital watermark, header, metadata and encryption system.

33. (original): A method of providing copy protection for protected media content on a computer system, the computer system comprising an output port and an associated output buffer, and an input port and an associated input buffer, said method comprising:

obtaining first media content buffered in the output buffer;

obtaining second media content buffered in the input buffer; and

comparing the first media content buffered in the output buffer and the second media content buffered in the input buffer through correlation of the first media content with the second media content, wherein a copy operation is modified or disabled when the correlation of the first media content and the second media content indicates that the first media content and the second media content match or otherwise coincide.

34. (original): The method of claim 33, wherein the correlation makes use of a transform domain.

35. (original): The method of claim 34, wherein the transform domain comprises a Fourier domain.

36. (original): The method of claim 35, wherein the first media content and the second media content each comprise audio.

37. (original): The method of claim 33, further comprising compensating for a time delay associated with the second media content relative to the first media content.

38. (original): The method of claim 34, further comprising compensating for a time delay associated with the second media content relative to the first media content.

39. (previously presented): A method of providing copy control for protected media content comprising:

determining which out of a plurality of copy control systems applies to the protected media content, said protected media content comprises a digital watermark embedded therein according to a key, said determining determines which out of a plurality of

copy control systems applies to the protected media content based on the key; and

controlling the protected media content according to a determined copy control system.

40. canceled.

41. (previously presented): The method of claim 39 wherein the key further designates a copy control state.

42. (previously presented): The method of claim 41, wherein the copy control state comprises at least one of copy never, copy once, copy freely or copy no more.

43. (previously presented): The method of claim 39 wherein the key indicates at least one of an embedding protocol, a watermark payload encryption scheme, an embedding characteristic, a pseudo-random sequence that is used to embed the watermark, locations within the media content used for watermark embedding, media content features to be modified to effect embedding or semantic meaning of particular features of the media content.

44. (previously presented): The method of claim 39 wherein each of the plurality of copy control systems corresponds to at least one unique key.

45. (previously presented): The method of claim 39, wherein the digital watermark comprising a multi-bit payload, and wherein said determining determines which out of a plurality of copy control systems applies to the protected media content based on at least one bit of the multi-bit payload and on the key.

46. (original): The method of claim 45, wherein each of the plurality of copy control systems is associated with a unique sequence of bits.

47. (currently amended): The method of claim 39, wherein the plurality of copy control systems comprises at least one of a DVD system or a conditional access TV system.

48. (original): A method of providing copy control for protected media content, the protected media content comprising a digital watermark embedded therein according to a key, said digital watermark comprising a payload, said method comprising:

determining which out of a plurality of copy control states should govern the protected media content by reference to the watermark key;

determining which out of a plurality of copy control systems the content should be handled by reference to the watermark payload; and

providing copy control according to the determined copy control state through the determined copy control system.

EVIDENCE APPENDIX

(No Evidence)

RELATED PROCEEDINGS APPENDIX

(No Related Proceedings)